The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.12
USAP Incident Response and Management

Organizational Function	Information Resource Management	Policy Number	5000.12
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Review By	1 August 2006
Subject	Incident Response and Management	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Polar Research Support Section	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov/od/opp
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.polar.org/infosec/index.htm		

1. PURPOSE

This directive establishes a Computer Incident Response Capability (CIRC) program for information systems supporting the National Science Foundation (NSF) Office of Polar Programs (OPP) United States Antarctic Program (USAP). The CIRC establishes the methods used to respond to adverse events in a computer system or network caused by a failure of a security mechanism or an attempted or threatened bridge of these mechanisms. The Computer Incident Response Team (CIRT) is the central element of the program. The CIRT shall have the ability to detect and react quickly and efficiently to disruptions in normal processing caused by acts of nature, accidents or malicious threats. Members of the CIRT will have the adequate technical knowledge and expertise to respond to information security incidents quickly and efficiently, with the proper authorization for actions required. The USAP CIRT team shall be formed following NSF and federal guidelines.

2. BACKGROUND

Federal information technology regulations direct USAP information systems managers to plan and implement an incident response program. USAP information system integrity ensures the success of the science research mission by providing reliable global

communications to facilitate field experiments and exchange of data concerning the Antarctic region. It also protects government and private resources used to execute and administer mission activities, while allowing effective access to program information by the general public. An effective incident response program ensures the USAP meets its mission requirements while responding to incidents that threaten its operations.

3. GUIDING PRINCIPLES

- Incident response is an integral element of information systems operations throughout the USAP
- Incidents can affect the entire enterprise, and they require a coordinated response from all USAP participants to minimize their damage
- The incident response team will work to restore operations as quickly and safely as possible.

4. POLICY

The USAP will establish a Computer Incident Response Capability (CIRC) program to respond to and manage adverse activities or actions that threaten the successful conduct of science and operations in the USAP. The USAP CIRC will follow existing NSF and Federal CIRC (FedCIRC) guidelines. The USAP CIRC will include a Computer Incident Response Team (CIRT) to respond to and manage information security incidents. The USAP CIRT will include representatives from the various USAP constituent organizations, as appropriate.

4.1 Operational Definitions

4.1.1 Computer Incident Response Team (CIRT).

The CIRT is an incident response team established to respond to and manage an incident. The team consists of a team leader, augmented by technical experts familiar with the specific incident type, drawn from existing staff with appropriate training.

4.1.2 Incident.

Any activity that is a threat to the confidentiality, integrity, or availability of information resources, has the potential to undermine science or operations activities, presents legal issues related to sensitive data, or is a misuse of government information resources. Examples of incidents include the presence of viruses or other malicious software; network probes, attacks or penetration; exploitation of known or previously undisclosed vulnerabilities; denial of service, or the assumption of control of a information resource by an unknown or unauthorized user. Unplanned outages or equipment failures, by themselves, may not necessarily constitute an information security incident warranting activation of the CIRT. The NSF CIO or designated representative makes the final determination as to whether or not an activity or event qualifies as an incident.

4.1.3 Incident Management.

The process of identifying and detecting incidents, evaluating the threat presented, reporting incident specifics to appropriate management, implementing corrective actions, and closing out the incident with an after-action report. USAP Incident Management is conducted in concert with the NSF CIRT and makes use of all appropriate NSF policies, processes and procedures for incident management.

4.2 Computer Incident Response Team (CIRT)

The CIRT shall respond to adverse events in a computer system or network caused by a failure of a security mechanism or an attempted or threatened bridge of these mechanisms.

4.2.1 USAP CIRT.

The Computer Incident Response Team will be established at several layers within the USAP. For the entire USAP, the USAP Information Security Manager will establish a CIRT consisting of appropriate management and technical representatives from the various USAP organizations, including the prime contractor. The USAP CIRT team will coordinate the enterprise level response that may be required for an incident. Each USAP participant organization will appoint a CIRT leader. The CIRT leaders from each organization will comprise the USAP CIRT.

4.2.2 Operating Location CIRT.

Each operating location will establish a site CIRT with the site IT manager or senior IT lead as the team lead. The team shall consist of available subject matter experts, and may be augmented by participants at other locations if warranted. The site CIRT coordinates the response to incidents at its location. At each operating location, the USAP prime contractor provides the primary CIRT members and support structure. Other USAP organizations may support the team as required.

4.2.3 Team Composition.

The CIRT will consist of a team leader, usually the station IT manager or senior IT representative, and team members selected for their expertise and familiarity with the type of incident in progress. The CIRT members must be capable and willing to follow procedures while providing a professional interface to constituents. The team leader may include on the team, representatives from other USAP functional elements, such as the facilities managers, or property custodians as necessary.

4.3 Incident Response and Management

4.3.1 Incident Characteristics.

Using guidance from NSF and NIST, the USAP CIRC will establish guidelines to distinguish between an incident, an unscheduled maintenance activity or equipment

failure, or an unplanned outage. The USAP IT operations staff will identify the characteristics of potential incidents based on trends analysis of routine information processing activities and comparison with industry standards and best practices.

4.3.2 Incident Response Timelines.

The Incident Response and Management process will include a timeline for incident management, which includes, at a minimum, timelines for declaring an activity to be a reportable incident, declaring an incident to be a disaster, and declaring an incident to be over.

4.3.3 Criminal Activity.

Because all aspects of an incident cannot be known from the outset, each incident is to be treated as a hostile action against the government's information resources. The CIRT leader will ensure the team follows proper procedures related to forensics issues, such as identification of possible criminal activity, and evidence protection. When necessary, the NSF CIRT may invite NSF OIG and federal law enforcement agencies to assist the team with these procedures.

4.3.4 Threat Awareness.

The USAP IT operations staff, as the primary manager of USAP information resources, will subscribe to appropriate federal CIRC notification services, as identified by the USAP Information Security Manager. This will ensure the IT operations team remains aware of current and potential threats.

4.3.5 Reporting and Notification.

The USAP CIRT will notify the NSF CIRT and OPP when an activity or event occurs which may meet NSF incident criteria. The CIRC will include a notification process with an escalation decision matrix to aid the CIRT in making reporting decisions. The CIRC will include provisions for completing after action reports, and for providing secondary notifications of the incident and results.

4.3.6 Organizational Procedures.

Each USAP participant organization will establish procedures for incident response and handling to implement federal government requirements for a CIRC. Procedures should follow NIST or DoD guidelines. All organizations will furnish a copy of their procedures and updates annually to the USAP Information Security Manager.

4.3.7 Internal Incident Handling.

Each USAP organization will handle incidents internal to their organization. If the incident affects any USAP information resource, the organization must report the incident to the USAP CIRT for follow-on reporting to NSF.

4.3.8 Incident Management.

The CIRT will maintain a log of all activities related to a particular incident. Standard procedures for administration and record-keeping will apply to the team's management of an incident.

4.3.9 Root Cause Analysis.

The team will conduct a root cause analysis of the incident as part of its incident closeout process. One aspect of the root cause analysis will be to determine if an individual's activities or actions created or contributed to the incident. The team will identify changes in processes, procedures, or other matters that may be required to prevent a reoccurrence. The team's report is not intended to affix blame or identify disciplinary actions.

4.3.10 Personnel Action.

In the event a participant is identified as having caused an incident, that participant's organization shall handle disciplinary action, and advise the NSF OPP Technical Manager of actions taken.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Security Policy 5000.1, *The USAP Information Security Program*.

6. RESPONSIBILITIES

6.1 NSF Director of Polar Programs

The NSF Director of Polar Programs ensures a comprehensive cost-effective security program is in place to protect NSF USAP information systems. After an information security incident, the Director of Polar Programs, as Certification Official for USAP information systems, approves or denies resumption of system operations based on CIRT recommendations.

6.2 NSF Technology Development Manager

Acts as official system manager for the USAP Enterprise and represents the USAP on the NSF and other federal CIRTs.

6.3 USAP Information Security Manager

The USAP Information Security Manager manages the CIRC program and the USAP CIRT. The ISM will establish processes and procedures for enterprise incident response

and management and composition of the incident response team. The ISM supports the development of procedures by each USAP organization, and maintains awareness of the external threat environment. The ISM coordinates CIRT activities across the various USAP organizations, and with the NSF CIO and NSF CIRT.

6.4 USAP Participant Organizations

Each USAP participant organization has a significant role in the successful response and handling of information security incidents. The USAP IT operations organization provides the technical expertise at the core of the CIRT, and its technicians and operators are usually the first to note activities that may turn into incidents. For the USAP CIRC, the USAP IT staff will provide technical and administrative support as required by the CIRT leader. The IT operations team will maintain awareness of the information environment's routine activities to identify abnormalities that might become incidents. The IT operations team will maintain awareness of external threats, and keep abreast of new technologies that can improve incident response. Other IT elements will bring potential incidents to the attention of the USAP ISM.

7. POLICY IMPLEMENTATION.

7.1 Guiding Standards.

The USAP CIRC will be based on existing federal and NSF directives, and will forward a copy of all policies, processes and procedures to the NSF CIRT..

7.2 Publication of CIRC Procedures.

Each USAP organization will publish internal procedures for implementing this policy, and provide copies to the USAP Information Security Manager. The USAP IT staff procedures shall implement NSF Manual 7 and appropriate federal regulations.

7.3 Policy Review.

The USAP Information Security Program Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP

8. AUTHORITY

Publication of this policy is in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002 and NSF Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director